

#2  
PMB  
5-29-02

Attorney Docket No. 1602.1006

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:

Satoshi MUKOGAWA

Application No.:

Group Art Unit:

Filed: December 17, 2001

Examiner:

U.S. PTO  
10/020434  
12/18/01

For: INFORMATION PROCESSING APPARATUS AND INPUT OPERATION APPARATUS

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN  
APPLICATION IN ACCORDANCE  
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s)  
herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2001-254509

Filed: August 24, 2001

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing  
date(s) as evidenced by the certified papers attached hereto, in accordance with the  
requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: December 17, 2001

By: 

James D. Halsey, Jr.  
Registration No. 22,729

700 11th Street, N.W., Ste. 500  
Washington, D.C. 20001  
(202) 434-1500

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

J1073 U.S. PTO  
10/020434  
12/18/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office

出 願 年 月 日

Date of Application:

2001年 8月24日

出 願 番 号

Application Number:

特願2001-254509

出 願 人

Applicant(s):

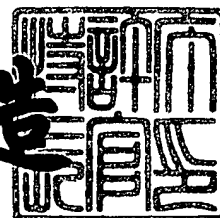
富士通株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年10月 4日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3090802

【書類名】 特許願

【整理番号】 0151102

【あて先】 特許庁長官殿

【国際特許分類】 H04K 1/02  
H04L 9/00

【発明の名称】 情報処理装置及び入力操作装置

【請求項の数】 8

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 向川 聡

【特許出願人】

    【識別番号】 000005223

    【氏名又は名称】 富士通株式会社

【代理人】

    【識別番号】 100097250

    【弁理士】

    【氏名又は名称】 石戸 久子

【選任した代理人】

    【識別番号】 100101856

    【弁理士】

    【氏名又は名称】 赤澤 日出夫

【手数料の表示】

    【予納台帳番号】 038760

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

特 2 0 0 1 - 2 5 4 5 0 9

【包括委任状番号】 0014371

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置及び入力操作装置

【特許請求の範囲】

【請求項 1】 操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、

前記入力操作部は、前記入力操作部より入力されるデータのうち、暗号化すべきデータを判別する暗号化判別手段と、前記暗号化判別手段の判別結果に基づき、暗号化すべきデータを暗号化する暗号化手段と、暗号化されたデータ、暗号化されないデータの双方を制御部に送信する送信手段とを有し、

前記制御部は、前記入力操作部より受信したデータにつき、暗号化されていないデータの内容に基づいた処理を行うとともに、暗号化されたデータを、復号化機能を有する装置に送信するよう制御することを特徴とする情報処理装置。

【請求項 2】 請求項 1 に記載の情報処理装置において、

前記入力操作部は入力操作画面を有し、

前記暗号化判別手段は、前記入力操作画面にて押下された座標が、所定の範囲又は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判別することを特徴とする情報処理装置。

【請求項 3】 請求項 2 に記載の情報処理装置において、

前記暗号化手段は、前記入力操作画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化することを特徴とする情報処理装置。

【請求項 4】 請求項 2 に記載の情報処理装置において、

前記入力操作画面における所定の座標範囲又は位置についての情報を外部装置より動的に受信し、設定する設定手段を有し、

前記暗号化判別手段は、前記入力操作画面にて押下された座標が、前記設定手段で設定された所定の範囲又は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判別するものであることを特徴とする情報処理装置。

【請求項 5】 請求項 3 に記載の情報処理装置において、

前記入力操作画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換するためのデータ設定情報を外部装置より動的に受信し、設定する設定手段を有し、

前記暗号化手段は、前記入力操作画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、前記設定手段に設定されたデータ設定情報に基づき、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化することを特徴とする情報処理装置。

【請求項 6】 入力操作画面を有し、該入力操作画面を通じて操作者より入力された情報を、接続された情報処理装置に提供する入力操作装置であって、

前記入力操作画面における所定の座標範囲又は位置についての情報、及び座標範囲又は位置において入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換するためのデータ設定情報を設定する設定手段と、

前記入力操作画面にて押下された座標が、前記設定手段で設定された所定の座標範囲又は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判別する暗号化判別手段と、

前記暗号化判別手段により暗号化すべきと判別された入力データにつき、前記設定手段に設定されたデータ設定情報に基づき、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化する暗号化手段と、

暗号化されたデータ、暗号化されないデータの双方を、接続された情報処理装置に送信する送信手段とを有することを特徴とする入力操作装置。

【請求項 7】 操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、

前記入力操作部は、入力された所定のデータを、入力操作部が有する所定のデータと比較する比較手段と、該比較手段により比較された比較結果を前記制御部に送信するための送信手段とを有し、

前記制御部は、受信した比較結果を他の装置に送信するよう制御することを特徴とする情報処理装置。

【請求項 8】 操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、

前記入力操作部は、所定のデータを入力する入力動作を検出する検出手段と、所定のデータを暗号化する暗号化手段と、前記検出手段による検出結果及び前記暗号化手段による暗号化データを前記制御部に送信する送信手段とを有し、

前記制御部は、受信した検出結果に基づき、前記入力操作部を制御するとともに、受信した暗号化データを、復号化機能を有する装置に送信するよう制御することを特徴とする情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、入力操作部と制御部を備えた装置に関し、特に、例えば金融機関端末や各種券売機等での入力操作を行う端末等に用いられる装置として、高いセキュリティを有する装置に関するものである。

【0002】

【従来の技術】

金融機関端末や各種券売機等において、タッチパネル等、画面上に表示されたボタンやポイントを実際に画面に触れる事によって操作する装置があるが、それらの装置にて暗証番号やクレジット番号等、操作者個人の秘密情報を入力する場合がある。また、それらの装置においては通常、入力操作部と装置制御部は一体化されておらず、それぞれがケーブル等で接続されている場合が多い。

【0003】

図 9 は、従来これら装置及び装置を含むシステムにおいてセキュリティが保証されていると考えられていた部分を示したブロック図である。本図は入力操作部 2 と、（装置）制御部 3 と、その他内部装置 6 とから構成される装置 1、装置 1 と専用線 7 で接続された外部機器 5 から構成されたシステムを示しており、図中の網掛部分がセキュリティが保証されていると考えられていた部分である。従って、入力操作部 2 から制御部 3 までのデータの伝達及び制御部 3 から内部装置 6 までのデータの伝達は平文（押下位置のポイントデータ等）で送受信されていた

。また、外部機器5に対しても専用線7により平文データで送受信されていた。

【0004】

【発明が解決しようとする課題】

ところが近年盗聴機器も高性能化してきており、また悪意を持つ者が装置1のメンテナンス作業者や係員になりすますことで不正が行われる場合もあり、必ずしも十分なセキュリティが保たれてはいるとは言えなくなってきた。このため装置1でタッチパネル等から暗証番号等の個人情報が入力された場合、個人情報が漏洩する危険が増大している。従ってこのような盗聴や不正に対応するため、装置内のセキュリティを向上させる必要がでてきている。更に現在、金融機関端末や各種券売機等は様々な場所に設置されているが、その設置場所が無人の場合も多い。またそうした装置の稼働時間も24時間もしくは深夜までといったように延長される傾向があり、装置における個人情報漏洩を防ぐための高いセキュリティの実現が求められてきている。

【0005】

装置のセキュリティを保つ手法としては、従来は特開平9-54862号公報や特開2000-20468号公報で示されるように、画面の覗き込み（盗み見）や動作解析によって前記秘密情報が漏洩する事を防ぐ方法が提案されている程度であるが、これらの手法では画面の操作位置及びキー配列が操作毎に変更されるため、操作者の慣れや利便性を阻害する恐れがある。

【0006】

また、セキュリティを保証するための単純な方法として、装置1のタッチパネル等での入力の際に、図10に示すようにタッチパネルで押された座標データをそのまま暗号化し、送信する方法が考えられる。本手法は、入力操作部2で入力された座標データ、例えば（2，7）が入力操作部2の暗号モジュール4で暗号化され、その暗号座標データ「eeff」が制御部3に送信される（S1）。データを受信した制御部3では暗号座標データの復号化を行い、座標データを画面構成に合わせ数値・文字データもしくは命令指示データに変換する必要がある。本例では数字「4」に変換される。ここで数字「4」について暗号化して外部機器5に送信すべきデータか否かを判別し、暗号化すべきデータと判別されれば数字



「4」を暗号化して、その暗号化電文「0dff」を外部機器5に送信する（S2）。数字「4」が暗号化すべきデータでない場合は暗号化せず、そのまま制御部内で処理されるか、暗号化しない生データをそのまま外部機器5に送信する、等の通常処理を行う（S3）。

【0007】

しかしながら該手法では制御部3でデータの解析を行うため、制御部3に対するセキュリティの保証及び盗聴防止機構（不正防止デバイス化）が必須となる。また制御部3で復号化／暗号化を行うため、復号化／暗号化用のモジュール（暗号モジュール4）も入力操作部2とは別に制御部3内に備えなくてはならない。更にまた暗号化する必要のない通常の制御データも入力操作部2から暗号化されて送信されるため、復号化の処理を行う分処理が増え、装置1に負荷がかかるという問題がある。

【0008】

本発明は、上述した事情に鑑みてなされたものであって、上記装置1内における個人秘密情報のセキュリティを確保して、他の外部装置へ安全に情報を伝達できる装置を提供する事を目的とする。

【0009】

【課題を解決するための手段】

上述した課題を解決するため、本発明は操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、前記入力操作部は、前記入力操作部より入力されるデータのうち、暗号化すべきデータを判別する暗号化判別手段と、前記暗号化判別手段の判別結果に基づき、暗号化すべきデータを暗号化する暗号化手段と、暗号化されたデータ、暗号化されないデータの双方を制御部に送信する送信手段とを有し、前記制御部は、前記入力操作部より受信したデータにつき、暗号化されていないデータの内容に基づいた処理を行うとともに、暗号化されたデータを、復号化機能を有する装置に送信するよう制御することを特徴とする情報処理装置を提供する。このような情報処理装置は、例えば金融機関等の端末や各種券売機などで使用される装置に適用される。なお、本実施の形態において、復号化機能を有する装置は外

部機器にあたる。

【0010】

また、前記暗号化手段は、前記入力操作画面にて押下された座標が、所定の範囲又は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判断することを特徴とする。このような構成によれば、例えば入力操作画面がタッチパネル式の画面である場合、操作者の押下した画面の座標範囲又は位置が例えばセキュリティを要する数字エリアであった場合には暗号化手段が暗号化し、セキュリティを要しない「取り消し」や「確認」のための入力エリアであった場合には暗号化しない等、場合に応じた対応が可能となり、効率よく処理することができる。

【0011】

更に、前記暗号化手段は、前記入力操作画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化することを特徴とする。具体的には、例えば上記と同様入力操作画面がタッチパネル式の画面である場合、操作者の押下した座標範囲や位置が数字エリアに相当する座標範囲や位置であった場合には該当の数字に変換するよう暗号化手段が機能する。更に変換された数字がセキュリティを要する場合には暗号化処理を行う。このような構成によれば、入力操作部で入力された様々なデータを適切なデータ情報に変換して利用することができ、さらに暗号化することでセキュリティを確実に確保することができる。

【0012】

更に、本発明に係る情報処理装置は、前記入力操作画面における所定の座標範囲又は位置についての情報を外部装置より動的に受信し、設定する設定手段を有し、前記暗号化判別手段は、前記入力操作画面にて押下された座標が、前記設定手段で設定された所定の範囲又は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判別するものであることを特徴とする。このような構成によれば、例えば入力操作画面がタッチパネル式画面である場合、タッチパネル画面のレイアウト等のような座標範囲や位置の情報を外部装置から受信し、

受信したデータに基づいて画面の設定を行うことができるため、様々なパターンでタッチパネルの表示を行うことができる。さらにそのようなレイアウトの情報に応じて暗号化の判別を行うことにより、様々なパターンに応じて暗号化処理を効率的に行うことが可能となる。

【0013】

更に又、本発明に係る情報処理装置において、前記入力操作画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換するためのデータ設定情報を外部装置より動的に受信し、設定する設定手段を有し、前記暗号化手段は、前記入力操作画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、前記設定手段に設定されたデータ設定情報に基づき、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化することを特徴とする。データ設定情報は、本発明の実施の形態4においては座標範囲及び関連データコードとの対応を示す座標情報（図5）により構成される。暗号化手段（実施の形態ではデータ処理部）は、該座標情報を用いてタッチパネルより入力されたデータを関連データコードに変換し、暗号化する。

【0014】

このような構成によれば、入力操作部の座標範囲や位置に対応して様々なデータを割り当てることができ、セキュリティを要する装置にあっては入力操作画面に対し多種多様な状況に応じた設定を施すことが可能となる。さらに該設定に応じて暗号化の処理がなされるため、従来に比して柔軟性高く、セキュリティを確保することができる。

【0015】

また、本発明は、入力操作画面を有し、該入力操作画面を通じて操作者より入力された情報を、接続された情報処理装置に提供する入力操作装置であって、前記入力操作画面における所定の座標範囲又は位置についての情報、及び座標範囲又は位置において入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換するためのデータ設定情報を設定する設定手段と、入力操作画面にて押下された座標が、前記設定手段で設定された所定の座標範囲又

は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判別する暗号化判別手段と、前記暗号化判別手段により暗号化すべきと判別された入力データにつき、前記設定手段に設定されたデータ設定情報に基づき、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化する暗号化手段と、暗号化されたデータ、暗号化されないデータの双方を、接続された情報処理装置に送信する送信手段とを有することを特徴とする入力操作装置を提供する。このような入力操作装置をセキュリティを要する金融機関等のシステムや各種券売機等の装置に設けることにより、従来に比してセキュリティが強化され、情報の漏洩を防止することができる。

## 【 0 0 1 6 】

また、本発明は操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、前記入力操作部は、入力された所定のデータを、入力操作部が有する所定のデータと比較する比較手段と、該比較手段により比較された比較結果を前記制御部に送信するための送信手段とを有し、前記制御部は、受信した比較結果を他の装置に送信するよう制御することを特徴とする。本発明の実施の形態では、入力操作部の内部メモリに予め会員番号の比較検証のための比較データを記憶しておき、例えば利用者が会員番号等をタッチパネルにて入力する際、その比較データと利用者により入力された会員番号を入力操作部にて比較検証して、その利用者が会員として登録されているか否かを判断するようにしている。

## 【 0 0 1 7 】

このような構成によれば、利用者が装置に対して入力した個人情報が外部に漏洩せず、セキュリティを確保できる。更に、入力されたデータについては入力操作部にて暗号化すべきか否かの判断がなされるため、暗号化及び復号化の処理を制御部で行う必要がなくなり、又装置内で行われる暗号化・復号化の処理を軽減することができる。これにより装置の負荷が軽減する。

## 【 0 0 1 8 】

更に、本発明は、操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、前記入力操作部

は、所定のデータを入力する入力動作を検出する検出手段と、所定のデータを暗号化する暗号化手段と、前記検出手段による検出結果及び前記暗号化手段による暗号化データを前記制御部に送信する送信手段とを有し、前記制御部は、受信した検出結果に基づき、前記入力操作部を制御するとともに、受信した暗号化データを、復号化機能を有する装置に送信するよう制御することを特徴とする。

## 【 0 0 1 9 】

例えば、一般的に金融機関等の端末のような装置において暗証番号の入力を行う場合、入力された番号自体は画面に表示されず、入力された旨を示す記号（例えば「\*」）のみが各数字が入力される度に表示されるようになっている。この場合、従来では入力操作部が押下された座標データを暗号化する等して制御部に送信することで制御部が入力動作を検出し表示画面を制御していたが、本発明に係る実施の形態では、入力操作部にて入力動作を検出するようにし、入力操作部から制御部に対して暗証番号の入力動作があったことのみを通知するだけで、制御部が表示画面を制御できるようにし、更に全ての暗証番号の数字の入力が完了した場合には、その暗証番号を暗号化して制御部に送信するようにしたため、従来に比して暗号化等の手間が省け、セキュリティも向上する。

## 【 0 0 2 0 】

## 【発明の実施の形態】

以下、図を用いて、本発明の実施の形態を詳細に説明する。

## 実施の形態 1.

図 1 は、本発明の一実施の形態における基本構成及びセキュリティ保証のための基本手法を簡便に表したブロック図である。上述した図 1 0 による手法と比較するため、図 1 0 と同様のデータを用いて説明する。図において、装置 1 0 は図 1 0 における装置 1 と同様に入力操作部 2 0 及び制御部 3 0 から構成され外部機器 5 0 に接続されている。

## 【 0 0 2 1 】

本手法は、まず入力操作部 2 0 でタッチパネルなどにより座標データ、例えば（2，7）が入力されると、押下座標（2，7）を関連データに変換する。ここでいう関連データとは、タッチパネルで押下された座標上に表示された数字など

の文字や記号等をいう。ここで関連データが数字「4」であるとする、入力操作部20において数字「4」が暗号化すべきデータか否かを判断し、暗号化すべきデータであると判断された場合には、入力操作部20の暗号モジュール24で数字「4」が暗号化され、その暗号化電文「0dff」が制御部30に送信される（S1a）。制御部30では受信したデータが暗号化電文であれば、何も処理を行わず受信した暗号化電文そのままを外部機器50に送信する（S1b）。

## 【0022】

また、同様に、入力操作部20で座標データ（2，7）が入力されると、押下座標（2，7）の変換された関連データが暗号化されるべきデータか否かを判断し、暗号化しなくてもよい、所謂平文で通信が可能であるデータだと判断された場合には、平文で座標データ（2，7）がそのまま制御部30に送信され（S2a）、通常処理される（S2b）。

## 【0023】

このような手法を用いることにより、特に、図9に示された装置1のように装置1全体もしくは入力操作部2と制御部3を一体化し、不正防止デバイスとしてセキュリティを確保できない場合、及び、物理的に入力操作部2とセキュリティを必要とされるデバイスが離れている場合であっても、本実施の形態に示された入力操作部20のように、暗号化すべきデータの識別機能を有していさえすれば、制御部3に暗号モジュール4を備える必要もなく、セキュリティを容易に確保できる。

## 【0024】

実施の形態2.

図2は本発明における実施の形態2の基本構成を示すブロック図である。図に示されるように、金融機関端末や各種券売機等の装置10は、利用者の入力操作コントロール及び暗号化やデータ送信等を行う入力操作部20及び装置10全体の制御を行いICカード等のセキュリティが保証されたデバイス（セキュリティモジュール）40や外部機器50に対してデータの送信を行う制御部30から構成される。

## 【0025】

入力操作部 2 0 は、タッチパネル等の入力部 2 1、入力部 2 1 による入力を制御する入力部コントローラ 2 2、入力部コントローラ 2 2 から入力データを受け取り座標データを所定のデータに変換したり暗号化のための符号化やブロック化を行うデータ処理部 2 3、データ処理部から受け取ったデータを暗号化する暗号モジュール 2 4、各種データを保存する内部メモリ 2 5、制御部 3 0 とのデータの送受信を行う送受信部 2 6 から構成される。

## 【 0 0 2 6 】

制御部 3 0 は、入力操作部 2 0 やセキュリティモジュール 4 0 や外部機器 5 0 とのデータの送受信を行うための送受信部 3 1、送受信部 3 1 により受信された座標データを所定のデータに変換するデータ変換部 3 2、入力部 2 1 の画面制御を行う画面表示制御部 3 3 から構成される。

また、図中の入力操作部 2 0 をはじめとする網掛部分はセキュリティが保証されているモジュール（不正防止デバイス）とする。

## 【 0 0 2 7 】

図 3 は、画面表示制御部 3 3 により制御されるタッチパネル式入力画面の表示例である。図中の網掛部分は利用者が暗証番号や金額等を入力する際に触れる数字エリア 2 1 a であり、ここで入力されるデータはセキュリティが保証されるようにしている。また、本画面はそうしたセキュリティエリア 2 1 a の他に、利用者が入力操作を行った場合、その入力動作を利用者が確認できるよう「\*」のような所定の文字等が表示されるエリア 2 1 b と、利用者が行った入力操作を取り消すためのエリア 2 1 c と、入力操作をやり直すためのエリア 2 1 d を備えている。

## 【 0 0 2 8 】

このような構成に基づき、以下、図 4 のフローチャートを用いて暗号化処理についての詳細を説明する。本実施の形態では、利用者が装置 1 0 に対して個人の秘密情報の 1 つである 4 桁の暗証番号を入力する処理を行い、入力データのまま、もしくは符号化或いはブロック化して暗号化し、不正防止デバイスである外部機器 5 0 或いはセキュリティモジュール 4 0 まで送信する例を説明する。

## 【 0 0 2 9 】

まず、装置 1 0 の制御部 3 0 の画面表示制御部 3 3 により図 3 に示されるような画面を表示する (S 4 0 0)。また、図 3 の画面においてセキュリティが必要な座標範囲部分 (2 1 a) の情報を別途外部機器 5 0 から動的にデータとして受信し通知され、座標範囲指定及び関連データコードを設定する (S 4 0 1)。この場合の関連データコードは便宜的にそれぞれ数字とする。例えば 1 が表示されている座標範囲 (1 0 ~ 2 0, 2 0 ~ 4 0) がポイントされた場合はコード「1」、5 が表示されている座標範囲 (2 0 ~ 3 0, 4 0 ~ 8 0) がポイントされた場合はコード「5」とする。このような設定は内部メモリ 2 5 に格納される。

#### 【 0 0 3 0 】

図 5 は、受信された座標情報の一例を示すものである。受信された情報は暗号化されていても良く、暗号化されていた場合には (S 4 0 2、Y)、入力操作部 2 0 の暗号モジュール 2 4 において復号化され使用される (S 4 0 3)。また、暗号化されていない場合には (S 4 0 2、N)、受信された情報そのままを使用する。このように本実施の形態では、セキュリティを要する座標の情報を外部機器 5 0 から受信するようにしたが、予め入力操作部 2 0 の内部メモリ 2 5 に静的に記憶しておいてもよい。

#### 【 0 0 3 1 】

ここで利用者が図 3 のように表示された画面から入力部 2 1 により暗証番号を入力する操作を行う。入力操作を行うと、入力データは入力部コントローラ 2 2 に通知され、座標データに変換される。この入力操作によりセキュリティが必要な情報以外の座標がポイントされた場合は (S 4 0 4、Y)、通常通り制御部 3 0 に座標情報をそのまま通知し処理を行う。具体的には、例えば利用者が (6 0, 8 0) の座標を押下したとすると、入力部コントローラ 2 2 により、押下された座標は図 3 に示されたセキュリティを要する座標範囲 (数字エリア 2 1 a) 内ではないと判断され、座標情報をそのまま制御部 3 0 に通知する (S 4 0 5)。制御部 3 0 では送受信部 3 1 による受信した座標データをデータ変換部 3 2 にて関連データに変換し、ポイントされた位置の関連データが、例えば「取消」処理であれば (S 4 0 6、Y)、入力処理自体を終了する等 (S 4 0 7)、「やり直し」であれば (S 4 0 6、N)、保持されている内部メモリ 2 5 内のデータを削



除し最初から入力させる等の処理を行う。

【0032】

また、セキュリティが必要な情報の座標がポイントされた場合は（S404、N、及び、S408、Y）、座標情報の代わりに入力通知のみを知らせるコードを制御部30に通知する（S409）。通知を受けた制御部30は、利用者に対して、画面上に入力桁数がわかるように「\*」のような文字を図3の表示エリア21bに表示させるのと同時に、入力を知らせる音等で通知する制御を行う。また、データ処理部23は内部メモリ25に格納された図5の情報を参照してポイントされた座標を関連データコードに変換し、変換結果を内部メモリ25内に格納する。例えば、利用者により（15，30）の座標が入力されたとなると、関連データコード「1」が格納される。利用者の暗証番号入力が終了しない間は（S410、N）、S404からS410の処理を繰り返す。

【0033】

セキュリティが必要な情報の座標が4点入力されると、暗証番号の入力が終了したとして（S410、Y）、データ処理部23は内部メモリ25内にあるコード情報を編集してブロック化し（S411）、暗号モジュール24にて暗号化し（S412）、送受信部26により制御部30に送信する（S413）。なお、ブロック化を、例えばコードを入力順に上位の桁に当てはめ、入力されていないコードを「0」として8桁のブロック化を行うようにしてもよい。この場合、例えばコード「1」、「2」、「3」、「4」の順でポイントされたデータは、「12340000」となる。

【0034】

もちろん、このブロック化を必ず行う必要はなく、符合化したり、また何の処理もせず暗号化のみを行うようにしてもよく、その処理は限定されない。

暗号化は、内部メモリ25内に記憶してある鍵を使用して行われる。送信された暗号化データは制御部30を通じて、セキュアな外部機器50或いはセキュリティモジュール40まで送信される。この際制御部30で本暗号化データが解析される事はない。

【0035】

### 実施の形態 3.

本実施の形態の基本構成は、実施の形態 2 で示された図 2 と同様である。また、本実施の形態では、8桁の会員番号入力処理を行い、番号を入力操作部 20 において比較・確認することにより、会員として登録されているかどうかを検証する例を用いる。従って、本実施の形態では、内部メモリ 25 内には、利用者により入力された会員番号を比較・確認するための比較データが予め格納されているか、もしくは暗号化された比較データを外部装置 50 から動的に受信するものとする。更に、本実施の形態では、予め座標範囲／位置とそれに関連するデータを複数パターン内部メモリ 25 に格納しておき、本パターンを表示画面にあわせて装置 10 の管理者が任意に選択できるものとする。

#### 【0036】

図 6 は、本実施の形態における会員番号入力処理の詳細を示したフローチャートである。まず、装置 10 の制御部 30 の画面表示制御部 33 により会員番号入力用の画面を表示する（S600）。図 7（a）は本実施の形態における会員番号入力用画面の表示例である。また、図 5 に示されるような座標範囲部分及びそれに対応する関連データコードの情報を予め複数パターン内部メモリ 25 に登録しておく。図 7（b）、（c）、（d）は登録されたパターンの例であり、この場合 3 パターン登録されているものとする。図において網掛部分がセキュリティを要する入力エリアである。

#### 【0037】

次に装置 10 の管理者が、図 7（a）の画面におけるセキュリティが必要な座標範囲部分情報に合致するパターンを、登録してあるパターン（図 7（b）、（c）、（d））から選択し、座標範囲指定及び関連データコードを設定する。この場合図 7（b）のパターン 1 を選択する（S601）。パターン選択のための画面は、画面表示制御部 33 により管理者用の設定入力画面が別途用意されており、その設定入力画面にて行う（図示せず）。また、選択されたパターンによる座標範囲指定及び関連データコードの設定は、実施の形態 2 と同様に行われているものとする。本設定に基づいて、入力された座標データがセキュリティを要するか否かが判断され、その判断に基づいて処理される。

## 【0038】

具体的には、まず、利用者が図7(a)の入力画面から会員番号を入力する操作を入力部21により行う。入力操作を行うと、入力データは入力部コントローラ22に通知され、座標データに変換される。変換された座標データがセキュリティ確保の必要があるデータか否かを入力部コントローラ22が上記設定に従って判断し、セキュリティが必要な情報以外の座標がポイントされた場合は(S602、Y)、通常通り制御部30に座標情報をそのまま通知し(S603)、処理を行う。その処理(S604からS605)は、実施の形態2と同様であるため説明を省略する。

## 【0039】

また、セキュリティが必要な情報の座標がポイントされた場合(S602、N、及び、S606、Y)の処理(S607)も実施の形態2と同様であり、ポイントされた座標に対応した関連データコードを内部メモリ25内に格納する。利用者の会員番号入力終了しない間は(S608、N)、S602からS608の処理を繰り返す。

## 【0040】

セキュリティが必要な情報の座標が8点入力されると(例えば、ここでは便宜的に会員番号「DF8-5220」が入力されたものとする。)、会員番号の入力が終了したとして、データ処理部23は、内部メモリ25内に静的に比較データが存在する場合には(S608、Y、静的)内部メモリ25内にある比較データを用いて、入力されたデータとの比較を行う(S609)。また、動的に受信した暗号化された比較データを用いる場合には(S608、Y、動的)、受信した暗号化データを復号化し比較する方法(S610)もしくは、入力されたデータを暗号化して比較する方法(S611)を用いて比較を行う。入力データを暗号化する方法は、内部メモリ25に受信した比較データを暗号化した鍵と同じ暗号化鍵を予め記憶しておき、それを用いて暗号化する。比較する方法はいずれを用いてもよく、特に限定されない。

## 【0041】

以下、比較処理の例を示す。

1. 静的に内部メモリに記憶された比較データを用いる場合 (S 6 0 9)

入力データ : D F 8 - 5 2 2 0

↓ (比較) -----> OK

比較データ : D F 8 - 5 2 2 0

【 0 0 4 2 】

2. 動的に受信した比較データを復号化して用いる場合 (S 6 1 0)

入力データ : D F 8 - 5 2 2 0

↓ (比較) -----> OK

比較データ復号化 : D F 8 - 5 2 2 0

↑ (復号化)

受信比較データ : 2 3 4 8 8 9 0 2 2 1 3

【 0 0 4 3 】

3. 動的に受信した比較データを用いるが、入力されたデータの方を暗号化して比較する場合 (S 6 1 1)

入力データ : D F 8 - 5 2 2 0

↓ (暗号化)

入力データ暗号化 : 2 3 4 8 8 9 0 2 2 1 3

↓ (比較) -----> OK

受信比較データ : 2 3 4 8 8 9 0 2 2 1 3

【 0 0 4 4 】

このように比較検証された結果は、制御部 3 0 或いは制御部 3 0 を通して外部機器 5 0 やセキュリティモジュール 4 0 に通知される (S 6 1 2)。具体的には、同一であれば (上記 OK)、送受信部 2 6 より送信データとして検証成功コードを送信する。もし相違があれば、送受信部 2 6 より送信データとして検証失敗コードを送信する。従って本実施の形態では、入力されたデータは入力操作部 2 0 内にて処理され、外部には検証結果のみが通知される。

【 0 0 4 5 】

実施の形態 4.

本実施の形態の基本構成は、実施の形態 2 で示された図 2 と同様である。また

、画面表示例は、図7(a)の画面表示例と同様であるとする。本実施の形態では、装置10の管理者が16桁の暗号化／復号化用の鍵の入力処理を行い、入力された暗号鍵を用いて暗号化したデータを送信する例を用いる。

#### 【0046】

図8は、本実施の形態における暗号化用鍵入力処理の詳細を示したフローチャートである。まず、装置10の制御部30の画面表示制御部33により暗号化用鍵入力用の画面を表示する(S800)。また、実施の形態2と同様に、別途外部機器50から動的に座標範囲指定及び関連データコードの情報を受信し、設定する(S801～S803)。

#### 【0047】

さらに、実施の形態2と同様に、まず、管理者が図7(a)の入力画面から入力部21により暗号化用鍵を入力する操作を行う。この入力操作から入力が終了するまでのフロー(S804～S810)は実施の形態2と同様であるため説明を省略する。

#### 【0048】

セキュリティが必要な情報の座標が16点入力されると(例えば、ここでは便宜的に暗号化／復号化用の鍵「0123456789ABCDEF」が入力されたものとする。)、入力部コントローラ22により内部メモリ25内に格納される(S811)。格納された暗号化／復号化用の鍵を用いて、暗号モジュール24により内部メモリ25内に記憶されたデータもしくは外部機器50から動的に受信したデータの暗号化を行う(S812)。暗号化の例を下記に示す。

#### 【0049】

内部メモリ25内のデータ：402933

(動的受信データ：402933)

↓ (入力鍵：0123456789ABCDEFによる暗号化)

暗号化データ：9A234DF123102AEF

暗号化され制御部30に送信された暗号化データは、制御部30からセキュアな外部機器50或いはセキュリティモジュール40まで送信される(S813)

なお、暗号化の方法自体は本発明の目的の範囲ではないので、ここでの詳細な説明は省略する。

【 0 0 5 0 】

また、本実施の形態により入力され格納された暗号化／復号化用の鍵は、上述した全ての実施の形態において利用可能である。

【 0 0 5 1 】

以上、本発明の様々な実施の形態を説明したが、本発明は上述した実施の形態に限定されることはなく、本発明の要旨を逸脱しない範囲において適用可能であることはもちろんである。

【 0 0 5 2 】

（付記 1）操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、前記入力操作部は、前記入力操作部より入力されるデータのうち、暗号化すべきデータを判別する暗号化判別手段と、前記暗号化判別手段の判別結果に基づき、暗号化すべきデータを暗号化する暗号化手段と、暗号化されたデータ、暗号化されないデータの双方を制御部に送信する送信手段とを有し、前記制御部は、前記入力操作部より受信したデータにつき、暗号化されていないデータの内容に基づいた処理を行うとともに、暗号化されたデータを、復号化機能を有する装置に送信するよう制御することを特徴とする情報処理装置。

（付記 2）付記 1 に記載の情報処理装置において、前記入力操作部は入力操作画面を有し、前記暗号化判別手段は、前記入力操作画面にて押下された座標が、所定の範囲又は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判別することを特徴とする情報処理装置。

（付記 3）付記 2 に記載の情報処理装置において、前記暗号化手段は、前記入力操作画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化することを特徴とする情報処理装置。

（付記 4）付記 2 に記載の情報処理装置において、前記入力操作画面における所定の座標範囲又は位置についての情報を外部装置より動的に受信し、設定する

設定手段を有し、前記暗号化判別手段は、前記入力操作画面にて押下された座標が、前記設定手段で設定された所定の範囲又は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判別するものであることを特徴とする情報処理装置。

（付記 5）付記 3 に記載の情報処理装置において、前記入力操作画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換するためのデータ設定情報を外部装置より動的に受信し、設定する設定手段を有し、前記暗号化手段は、前記入力操作画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、前記設定手段に設定されたデータ設定情報に基づき、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化することを特徴とする情報処理装置。

（付記 6）入力操作画面を有し、該入力操作画面を通じて操作者より入力された情報を、接続された情報処理装置に提供する入力操作装置であって、前記入力操作画面における所定の座標範囲又は位置についての情報、及び座標範囲又は位置において入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換するためのデータ設定情報を設定する設定手段と、前記入力操作画面にて押下された座標が、前記設定手段で設定された所定の座標範囲又は位置にあるか否かに基づき、入力されたデータを暗号化するか否かを判別する暗号化判別手段と、前記暗号化判別手段により暗号化すべきと判別された入力データにつき、前記設定手段に設定されたデータ設定情報に基づき、その座標範囲又は位置に関連付けられるデータ情報に変換し、所定の鍵を使用して暗号化する暗号化手段と、暗号化されたデータ、暗号化されないデータの双方を、接続された情報処理装置に送信する送信手段とを有することを特徴とする入力操作装置。

（付記 7）操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、前記入力操作部は、入力された所定のデータを、入力操作部が有する所定のデータと比較する比較手段と、該比較手段により比較された比較結果を前記制御部に送信するための送信手段とを有し、前記制御部は、受信した比較結果を他の装置に送信するよう制御する

ことを特徴とする情報処理装置。

（付記 8）操作者により入力される入力操作部と、前記入力操作部に対して所定の制御を行う制御部とを備えた情報処理装置であって、前記入力操作部は、所定のデータを入力する入力動作を検出する検出手段と、所定のデータを暗号化する暗号化手段と、前記検出手段による検出結果及び前記暗号化手段による暗号化データを前記制御部に送信する送信手段とを有し、前記制御部は、受信した検出結果に基づき、前記入力操作部を制御するとともに、受信した暗号化データを、復号化機能を有する装置に送信するよう制御することを特徴とする情報処理装置。

（付記 9）付記 3 に記載の情報処理装置において、前記暗号化手段は、前記入力操作画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力されたデータを、その座標範囲又は位置に関連付けられるデータ情報に変換すると共に、該データ情報を符合化もしくはブロック化し、該符合化もしくはブロック化されたデータを所定の鍵を使用して暗号化することを特徴とする情報処理装置。

（付記 10）付記 7 に記載の情報処理装置において、前記入力操作部には、前記入力操作部より入力されるデータのうち、前記比較手段により比較すべきデータを判別する比較判別手段を備え、前記比較手段は前記比較判別手段により判別されたデータを比較することを特徴とする情報処理装置。

（付記 11）付記 7 に記載の情報処理装置において、前記入力操作部が有する所定のデータは、前記入力操作部が有するメモリ内に記憶されていることを特徴とする情報処理装置。

（付記 12）付記 7 に記載の情報処理装置において、前記入力操作部が有する所定のデータは、外部装置から暗号化されて送られる受信データに基づくデータであることを特徴とする情報処理装置。

（付記 13）付記 12 に記載の情報処理装置において、前記暗号化されたデータを復号する復号化手段を備えていることを特徴とする情報処理装置。

（付記 14）付記 12 又は付記 13 に記載の情報処理装置において、前記入力操作部は、前記入力操作部より入力されたデータを、前記外部装置から暗号化されて送られる前記受信データが暗号化されたものと共通の鍵により暗号化する手段



を有し、前記比較手段は、これら暗号化されているデータを比較することを特徴とする情報処理装置。

（付記 1 5）付記 1 0 に記載の情報処理装置において、前記入力操作部は入力操作画面を備え、前記比較判別手段により判別が行われて前記比較手段により比較処理が行われるデータは、前記入力操作画面における所定の座標範囲又は位置の少なくともいずれかにおいて入力され、その座標範囲又は位置に関連付けられるデータであることを特徴とする情報処理装置。

（付記 1 6）付記 5 に記載の情報処理装置において、前記外部装置から受信される前記データ設定情報は暗号化されており、前記入力操作部には、該暗号化された前記データ設定情報を復号化する手段を有することを特徴とする情報処理装置。

（付記 1 7）付記 5 に記載の情報処理装置において、互いに異なる複数の前記データ設定情報を記憶する記憶手段を有し、前記入力操作画面において、前記複数の設定情報の中から所定のデータ設定情報を選択して設定できる手段を有することを特徴とする情報処理装置。

（付記 1 8）付記 1 乃至付記 5 又は付記 1 3 のいずれかに記載の情報処理装置において、前記データを暗号化するための鍵、及びデータを必要に応じて復号化するための鍵は、前記入力操作部により入力された所定のデータに基づいて形成されることを特徴とする情報処理装置。

（付記 1 9）付記 1 乃至付記 5 又は付記 7 乃至付記 1 8 のいずれかに記載の情報処理装置において、前記入力操作部は不正防止デバイスで構成されていることを特徴とする情報処理装置。

（付記 2 0）付記 1 乃至付記 5 又は付記 7 乃至付記 1 9 のいずれかに記載の情報処理装置において、前記所定のデータは、セキュリティを要求されるデータであり、暗証番号やクレジット番号等、操作者個人の秘密情報、又は暗号化／復号化用の鍵等のデータの少なくともいずれかが含まれることを特徴とする情報処理装置。

【 0 0 5 3 】

【発明の効果】

以上説明したように、本発明は、入力操作部と制御部を有する装置において、入力操作部に入力されたデータを暗号化する暗号モジュールと外部機器に送信するための送受信部を備えたため、不正防止デバイスとして入力操作部と制御部が一体化できない場合や、物理的に入力操作部とセキュリティを要するデバイスが離れている場合であっても、個人情報漏洩せず、セキュリティを確保できる。更にまた、本発明は、入力操作部に入力されたデータを暗号化すべきか否かを判別するための機能を設けたことにより、制御部は入力操作部から受信したデータについて暗号化及び復号化の処理を行う必要がなくなり、装置内で行われる暗号化・復号化の処理を軽減することができるため、装置の負荷が軽減する。また、従来の装置を使用する場合においても、装置制御部側の変更を要せず、入力操作部の交換のみで対応できるため、既存設置装置に対しても導入コストの低減を計る事ができ、装置におけるセキュリティが大幅に向上する。

【図面の簡単な説明】

【図 1】

本発明の実施の形態 1 における基本構成及びセキュリティ保証のための基本手法を簡便に表したブロック図である。

【図 2】

本発明における実施の形態 2 乃至実施の形態 4 の基本構成を示すブロック図である。

【図 3】

タッチパネル式入力画面の表示例である。

【図 4】

実施の形態 2 における暗号化処理のフローチャートである。

【図 5】

セキュリティが必要な座標範囲とそれに対応する関連データの一例である。

【図 6】

実施の形態 3 における会員番号入力処理のフローチャートである。

【図 7】

(a) 実施の形態 3 及び実施の形態 4 における入力用画面の表示例である。

(b)、(c)、(d)は実施の形態2における登録された座標範囲部分及びそれに対応する関連データコードの情報のパターンの例である。

【図 8】

実施の形態4における暗号化用鍵入力処理の詳細を示したフローチャートである。

【図 9】

従来セキュリティが保証されていると考えられていた部分を示したブロック図である。

【図 1 0】

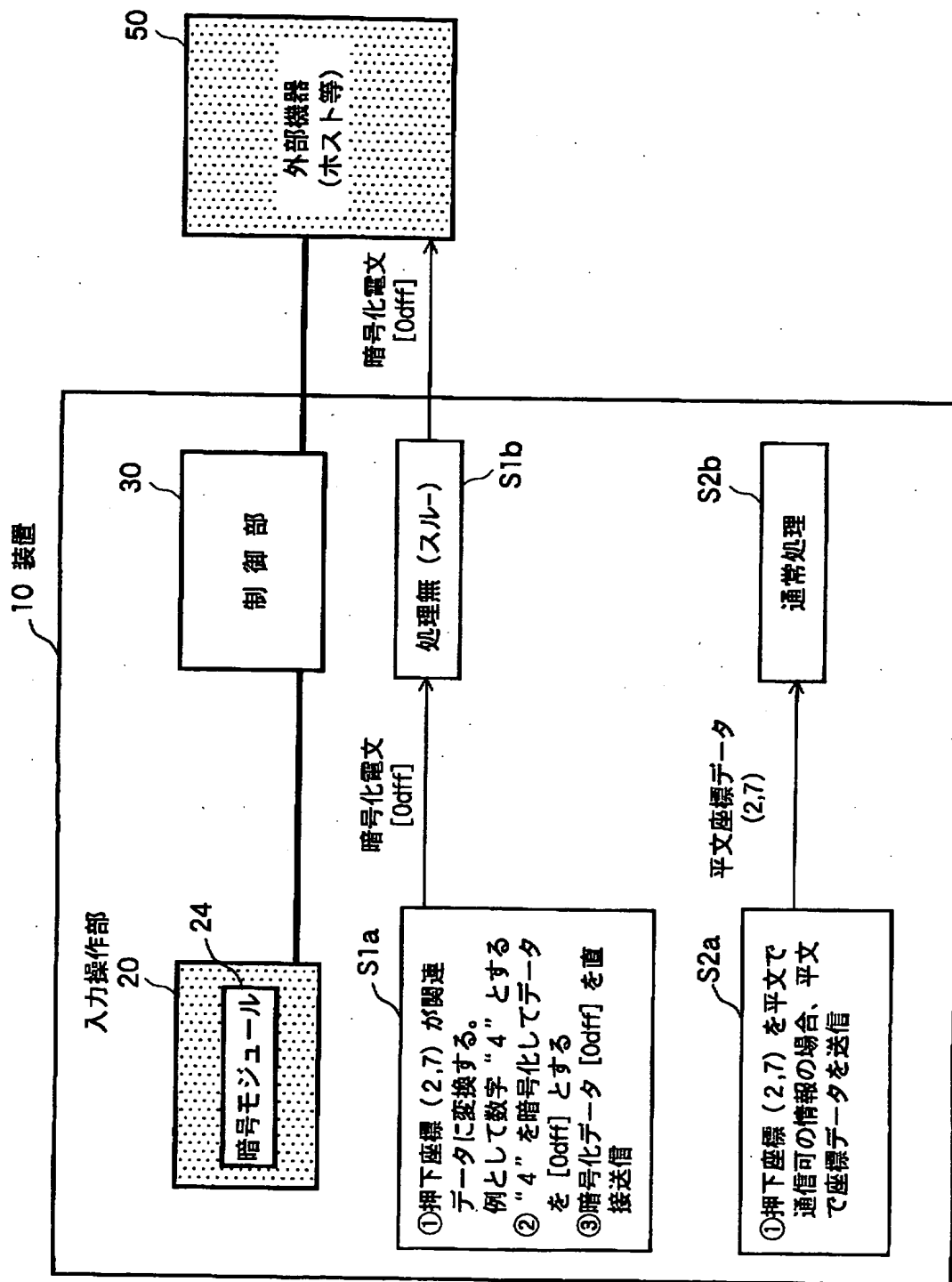
タッチパネルで押された座標データをそのまま暗号化し、送信する手法を示したブロック図である。

【符号の説明】

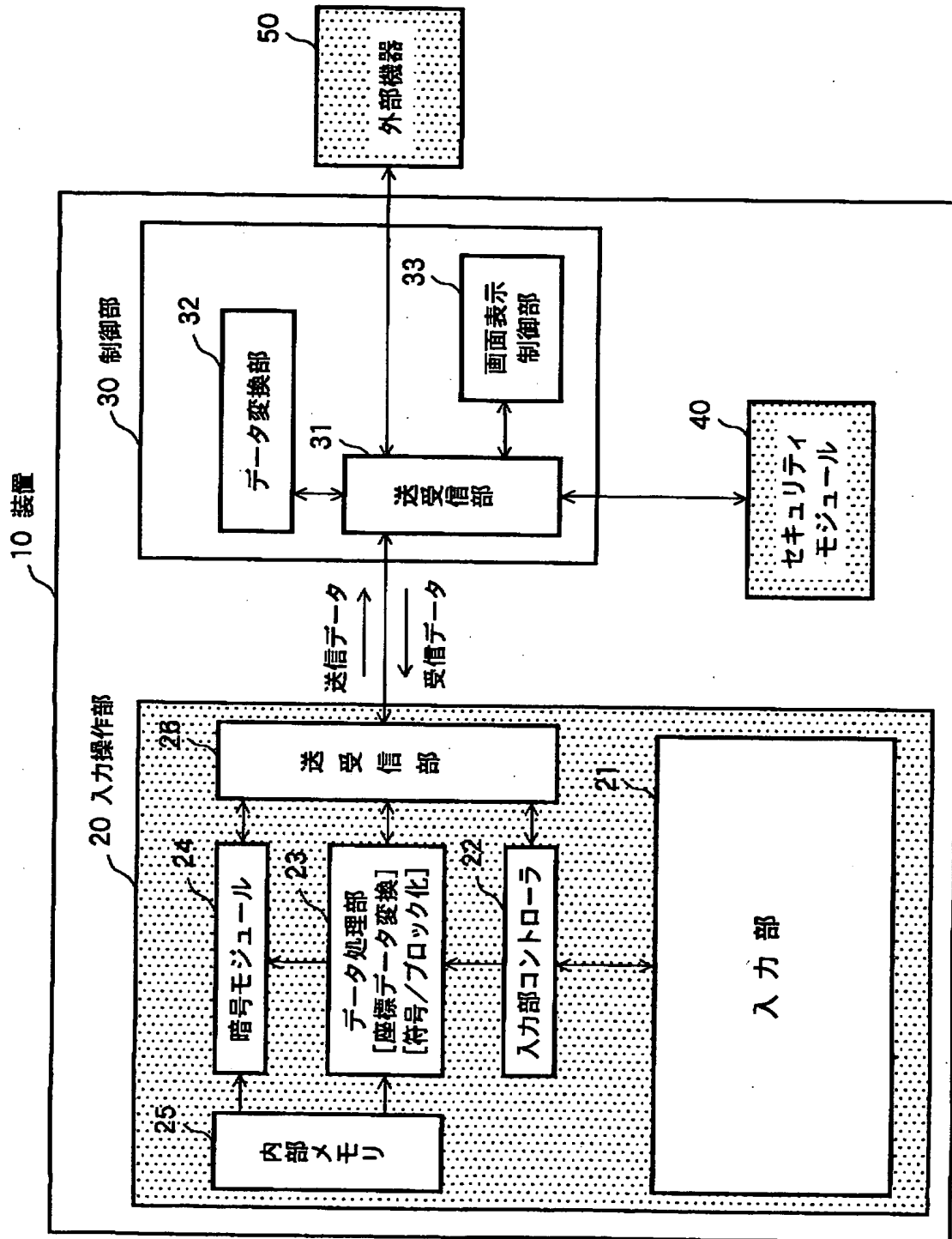
1 0 装置、2 0 入力操作部、2 1 入力部、2 2 入力部コントローラ、2 3 データ処理部、2 4 暗号モジュール、2 6 送受信部、3 0 制御部、3 1 送受信部、3 2 データ変換部、3 3 画面表示制御部、4 0 セキュリティモジュール、5 0 外部機器。

【書類名】 図面

【図 1】



【図2】



【図 3】

暗証番号を入力してください。

(10,20)	(20,20)	(30,20)	(40,20)
1	2	3	
(10,40)			
4	5	6	
(10,60)			
7	8	9	
(10,80)			
	0		
	(20,100)	(30,100)	

21a

21b

\*\*\*

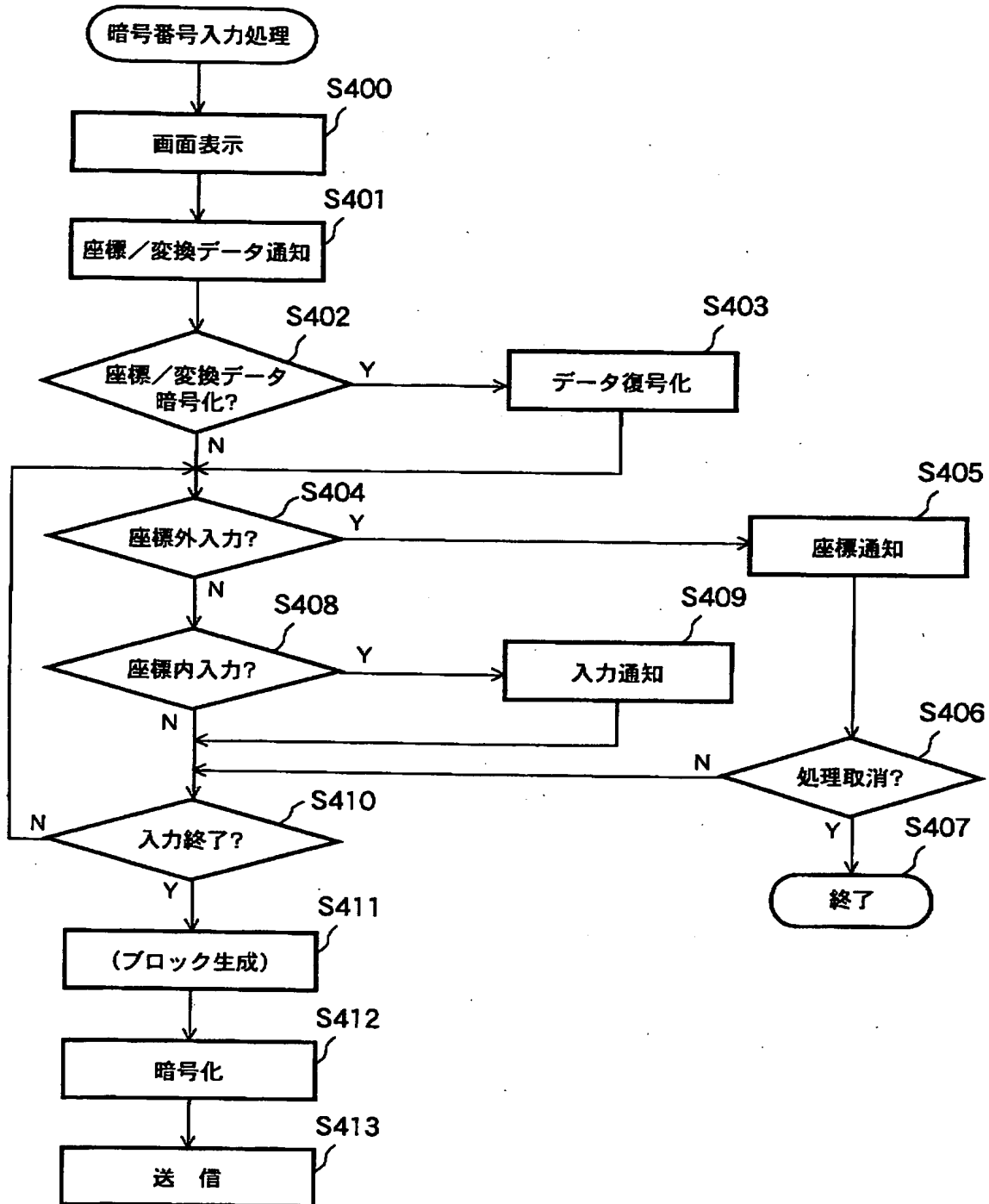
21c

取 消

21d

やり直し

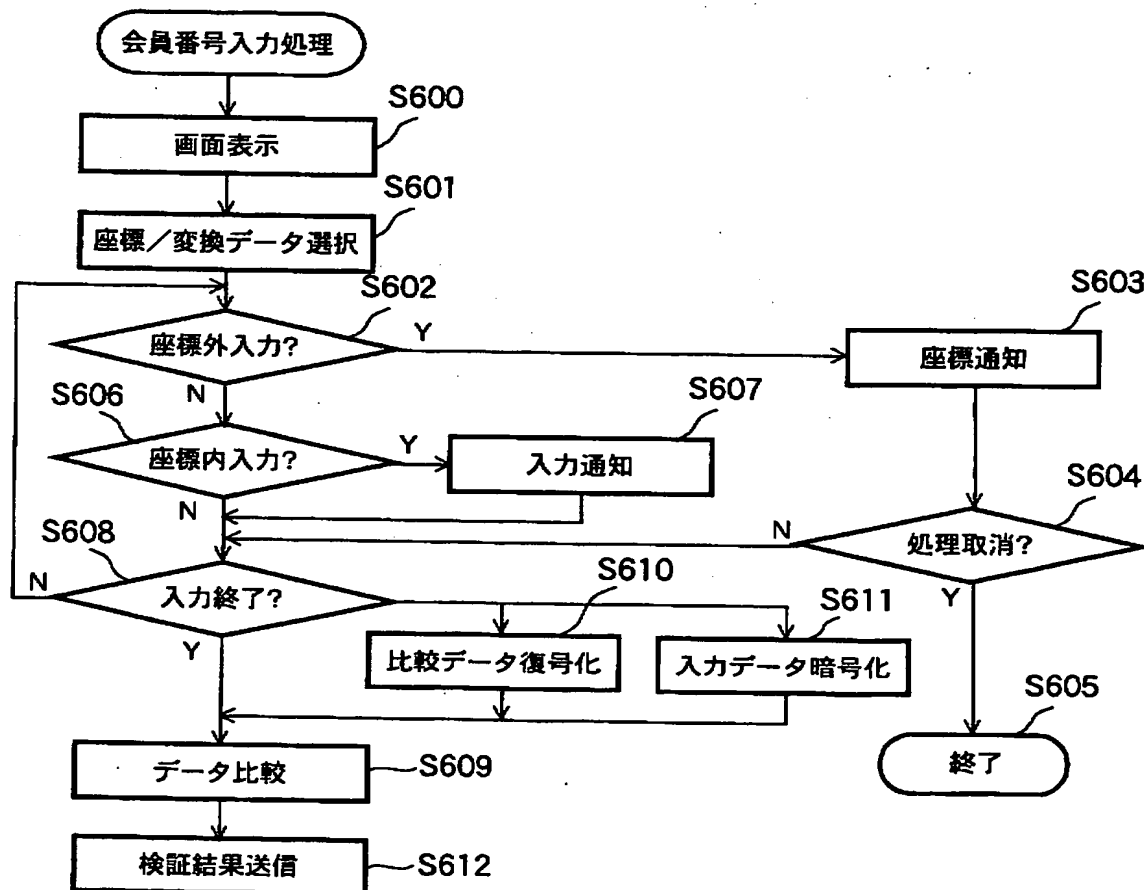
【図 4】



【図 5】

座標範囲		関連データ
X 座標	Y 座標	
(10~20)	(20~40)	1
(20~30)	(20~40)	2
(30~40)	(20~40)	3
(10~20)	(40~60)	4
(20~30)	(40~60)	5
(30~40)	(40~60)	6
(10~20)	(60~80)	7
(20~30)	(60~80)	8
(30~40)	(60~80)	9
(20~30)	(80~100)	0

【図 6】





【図 7】

(a) 画面表示例

会員番号を入力してください

\*\*\*\*\*

0	1	2	3	4	5	6	7	8	9	0
A	B	C	D	E	F					

(b) パターン1

0	1	2	3	4	5	6	7	8	9
A	B	C	D	E	F				

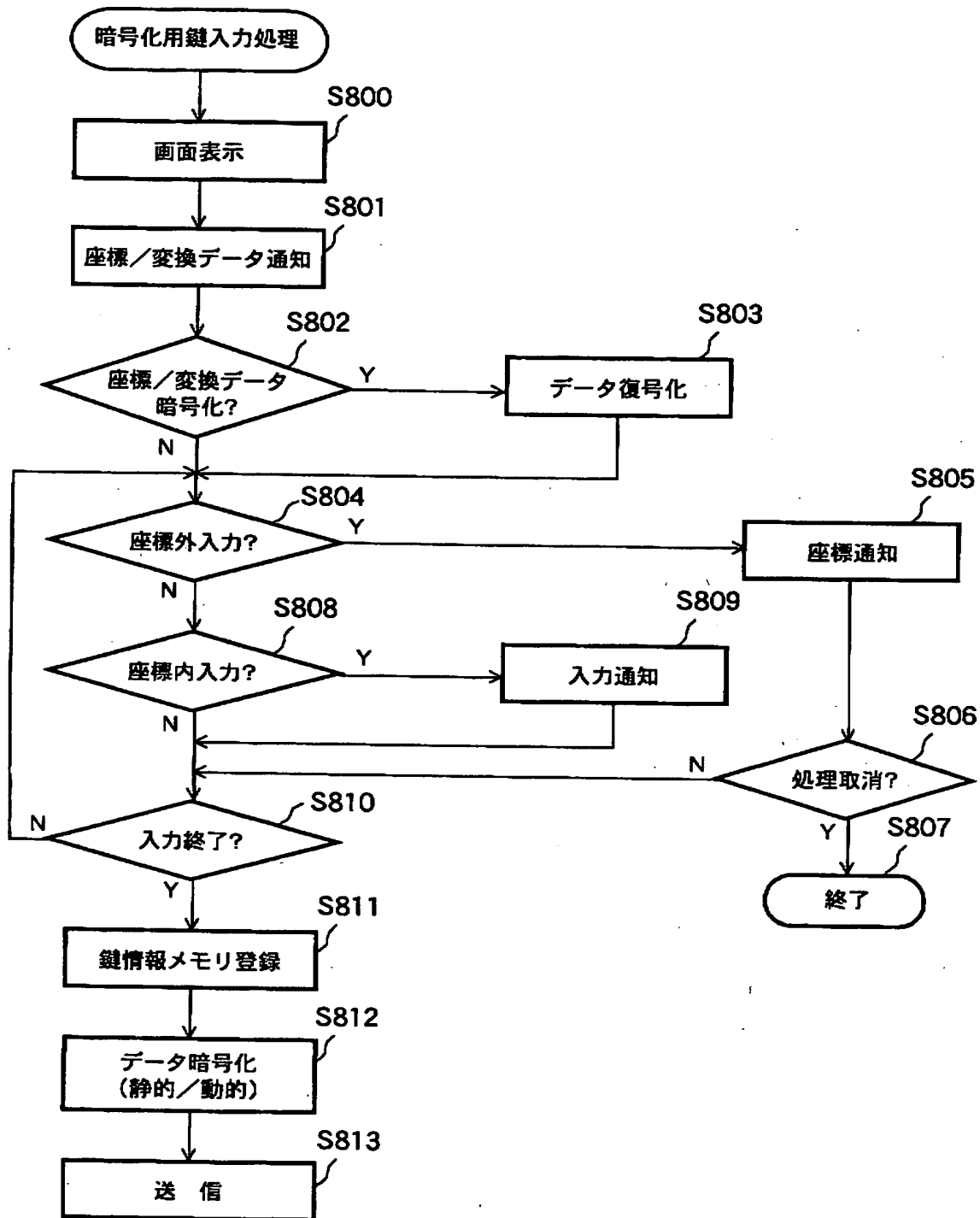
(c) パターン2

1	2	3
4	5	6
7	8	9
0		

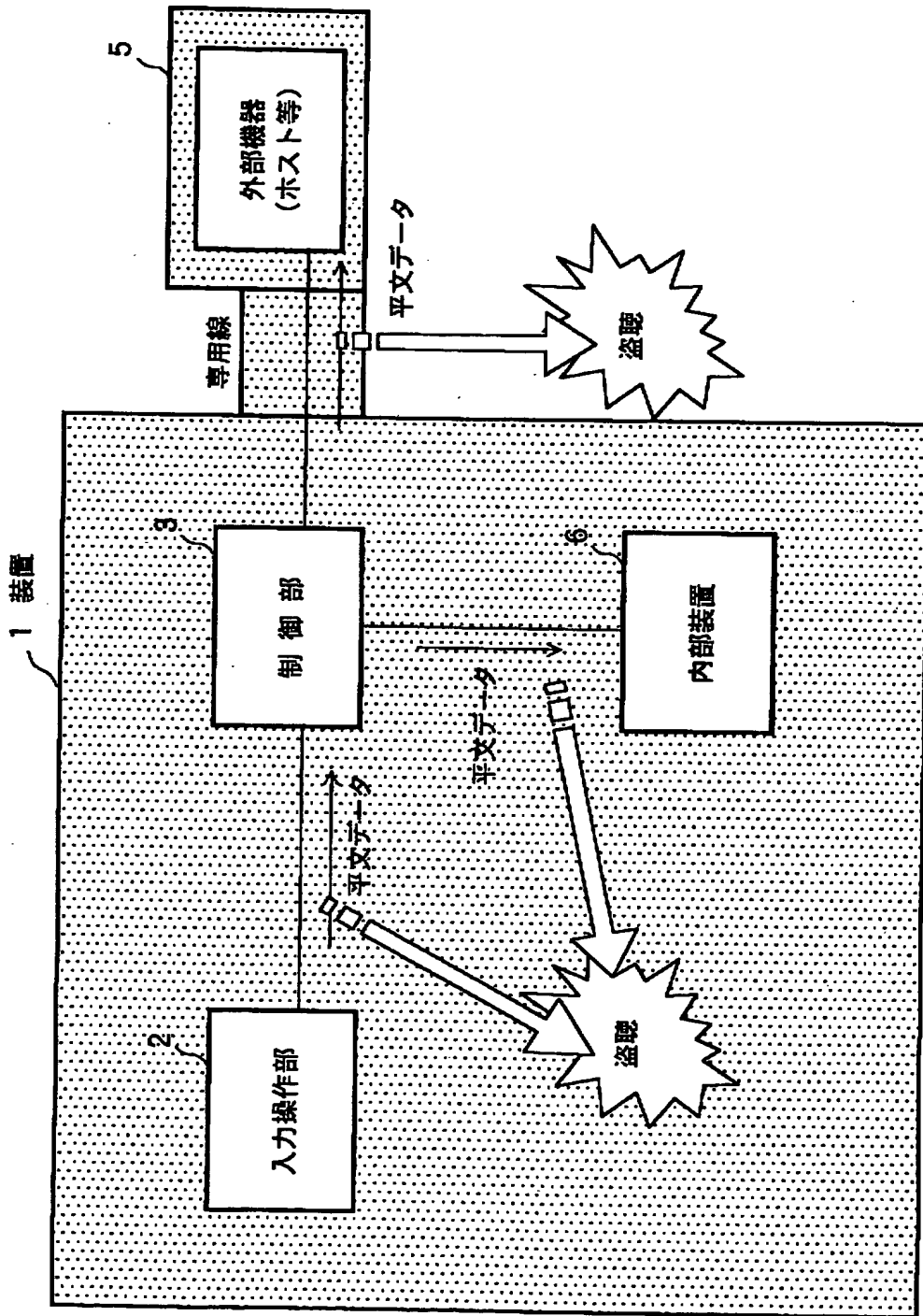
(d) パターン3

0	1	2	3	4	5	6	7	8	9
---	---	---	---	---	---	---	---	---	---

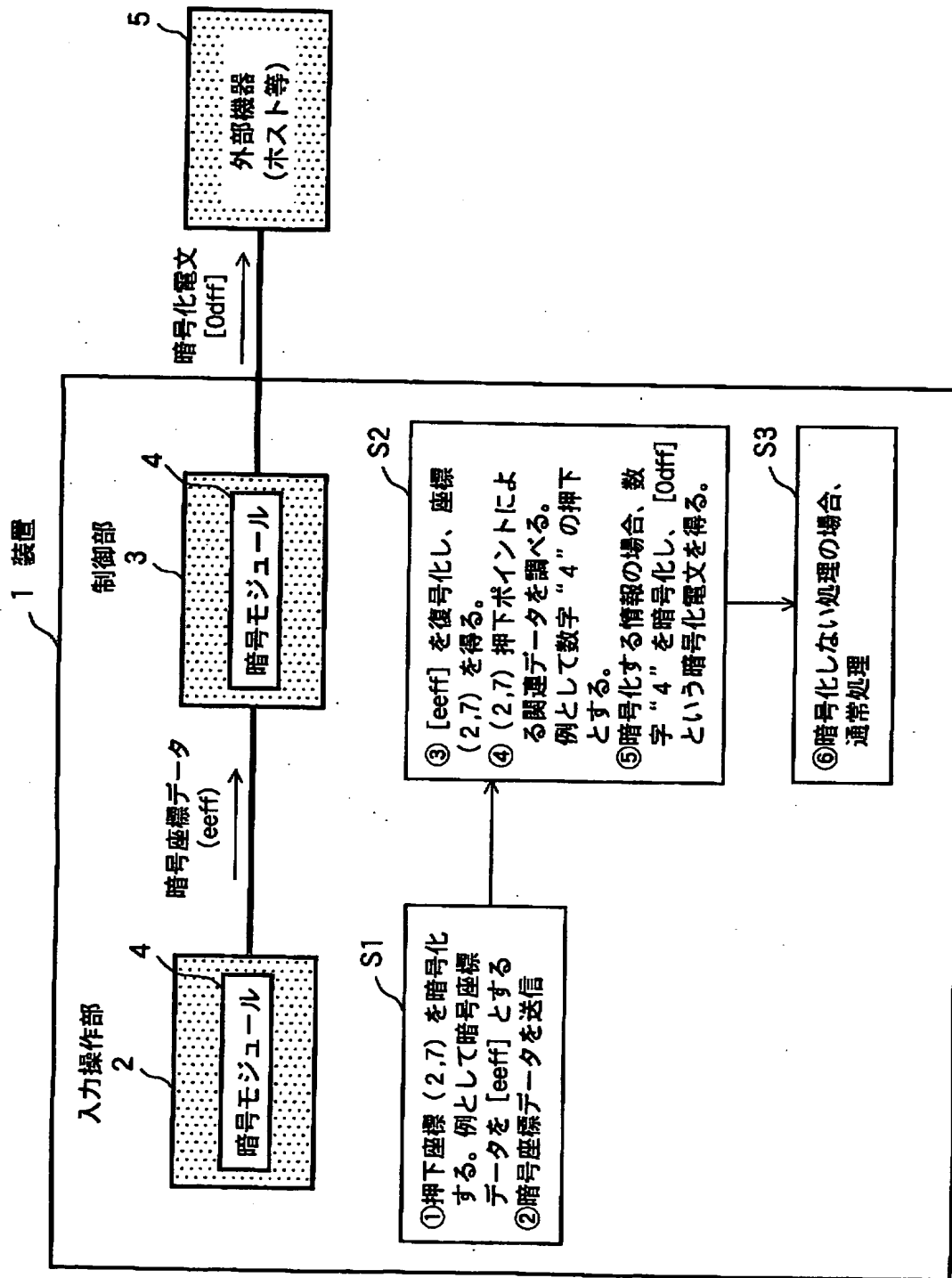
【図 8】



【図9】



【図10】



【書類名】            要約書

【要約】

【課題】    装置における個人情報漏洩を防ぎ、セキュリティを確保する。

【解決手段】    所定の入力操作を行う入力操作部 2 0 と、入力操作部 2 0 に対して所定の制御を行う制御部 3 0 とを備えた装置 1 0 であって、該装置 1 0 の外部に設けられる外部装置 5 0 とデータの送受信を行う入力操作部 2 0 を有する装置 1 0 において、入力操作部 2 0 に、該入力操作部 2 0 より入力された所定のデータを暗号化する暗号モジュール 2 4 と、該暗号モジュール 2 4 により暗号化されたデータを外部装置 5 0 に送信するための送受信部 2 6 を設けたことを特徴とする入力操作部 2 0 を有する装置 1 0 を提供する。

【選択図】            図 1

特2001-254509

認定・付加情報

特許出願の番号	特願2001-254509
受付番号	50101241212
書類名	特許願
担当官	第七担当上席 0096
作成日	平成13年 8月27日

<認定情報・付加情報>

【提出日】	平成13年 8月24日
-------	-------------

次頁無

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号  
氏 名 富士通株式会社